

installation and
reference guide

HP StorageWorks Secure Path 4.0C Service Pack 2 for Windows and Windows Workgroup Edition

Product Version: 4.0C SP2

Eighth Edition (March 2005)

Part Number: AA-RL4SJ-TE

This guide describes how to install HP StorageWorks Secure Path 4.0C Service Pack 2 for Microsoft Windows® and Windows Workgroup Edition, for use with Enterprise Virtual Array (HSV100, HSV110), Enterprise Modular Storage RAID Array (RA/MA8000, ESA/EMA12000, and EMA16000), Modular Smart Array 1000 (MSA1000) and Modular Smart Array 1500 (MSA1500), VA and XP disk array systems.



© Copyright 1999–2005 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Compaq Computer Corporation is a wholly-owned subsidiary of Hewlett-Packard Company.

Microsoft®, MS-DOS®, MS Windows®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the US.

Secure Path 4.0C Service Pack 2 for Windows and Windows Workgroup Edition installation and reference guide

Eighth Edition (March 2005)

Part Number: AA–RL4SJ–TE

Contents

About this Guide	1
Overview	2
Intended audience	2
Related documentation	2
Conventions	3
Document conventions	3
Text symbols	3
Equipment symbols	4
Rack stability	6
Getting help	7
HP technical support	7
HP storage Web site	7
HP authorized reseller	7
1 Installation prerequisites	9
Secure Path prerequisites	10
Installation and configuration information	11
Installation and configuration documentation	11
Supported SAN topologies	11
Installation and configuration checklist	12
2 Installing Secure Path software	13
Before you begin	14
Software installation types	15
New installations	15
New installations on standalone systems	16
New installations on cluster configurations	16
Upgrading on systems with previous versions of Secure Path	17
Upgrading from Windows NT 4.0	17
Upgrading from Windows 2000 to Windows Server 2003	17

Standalone servers	17
Clustered servers	18
Recovering from an unsuccessful upgrade	19
Upgrading from Windows 2000 to Windows Server 2003 on servers that boot from SAN-connected devices.	19
Standalone servers.	19
Clustered servers	20
Recovering from an unsuccessful upgrade	21
Upgrading Secure Path on systems with previous versions of Auto Path	21
Installing the Secure Path software.	22
Using silent installation	23
Silent installation for standard edition	24
Installing new Secure Path server	24
Updating installation	24
Silent installation for workgroup edition	25
Installing new Secure Path server	25
Updating installation	26
Uninstalling Secure Path server.	27
Installing Hs_Service	27
Bootting Secure Path servers from a Storage Area Network	28
Uninstalling Secure Path software	29
3 Managing storage arrays with the Secure Path CLI	31
Secure Path Manager CLI overview	32
Common terms	32
Configuration Information	33
Path states	33
Path Modes	34
Device States	34
Starting Secure Path Manager CLI	35
spmgr commands	36
Displaying information	38
Display header information	38
Display differences between controllers	38
HSG80 display	38
HSV110 display	38
MSA1000 display	39
XP display	39
VA display	39

The display command	40
spmgr display	40
spmgr display -c[v] [controller_serial_number]	42
spmgr display -d[v]	44
spmgr display -r[v] [WWNN]	48
The alias and unalias commands	52
spmgr alias alias_name old_name	52
spmgr unalias	53
spmgr alias	53
The password command	53
spmgr passwd agent_password	54
Setting storage system properties	55
The set command	55
spmgr set -a on off [WWNN]	55
spmgr set -b on off [WWNN]	55
spmgr set -b <type> [WWNN]	55
spmgr set -p on off [WWNN]	56
Path management	57
The select command	57
spmgr select -p [handle] [path_index]	57
spmgr select -c [handle] [controller_serial_number]	57
The repair command	58
spmgr repair -p [handle] [path_index]	58
The quiesce command	58
spmgr quiesce -p [handle] [path_index]	58
The restart command	59
spmgr restart -p [handle] [path_index]	59
4 Managing XP and VA arrays with the legacy Auto Path CLI	61
Starting Auto Path CLI	62
Auto Path CLI command summary	63
autopath adapters	64
autopath devices	65
autopath help	66
autopath paths device	67
autopath set device	68

A	Software components	69
B	Secure Path driver event log messages	73
	Informational messages for HSV, HSG, and MSA	74
	Event id = 257	74
	Event id = 513	74
	Event id = 514	74
	Event id = 515	75
	Event id = 516	75
	Event id = 520	76
	Event id = 521	76
	Event id = 523	77
	Event id = 524	77
	Event id = 525	77
	Event id = 526	78
	Event id = 527	78
	Event id = 528	79
	Event id = 790	79
	Warning messages for HSV, HSG, and MSA	80
	Event id = 769	80
	Event id = 770	80
	Event id = 771	81
	Event id = 772	81
	Event id = 773	82
	Event id = 774	82
	Event id = 775	82
	Event id = 776	83
	Event id = 777	83
	Event id = 778	84
	Event id = 779	84
	Event id = 780	85
	Event id = 781	85
	Event id = 782	86
	Event id = 784	86
	Event id = 785	87
	Event id = 786	87
	Event id = 787	87
	Event id = 788	88
	Error messages for HSV, HSG, and MSA	89

Event id = 256	89
Event id = 1025	89
Event id = 1026	90
Event id = 1027	90
Event id = 1028	91
Event id = 1029	91
Event id = 1030	92
Event id = 1031	92
Event id = 1032	93
Event id = 1033	93
Event id = 1034	93
Event id = 1035	94
Event id = 1036	94
Informational messages for XP and VA	95
Event id = 3	95
Event id = 4	95
Error messages for XP and VA	96
Event id = 1	96
Event id = 2	96
Event id = 5	96
Event id = 6	97
Event id = 7	97
Event id = 8	98
Glossary	99
Index	103
Figures	
Tables	
1 Document conventions	3
2 Secure Path installation prerequisites	10
3 Installation and configuration checklist	12
4 Spmgr common terms	32
5 Path states	33
6 Path modes	34
7 Device states	34

8	Spmgr commands.	36
9	Auto Path CLI commands	63

Tables

1	Document conventions	3
2	Secure Path installation prerequisites	10
3	Installation and configuration checklist	12
4	Spmgr common terms	32
5	Path states	33
6	Path modes	34
7	Device states	34
8	spmgr commands	36
9	Auto Path CLI commands	63

Figures

About this Guide

This installation and reference guide provides information to help you:

- Install Secure Path software for StorageWorks Enterprise Virtual Array (HSV100, HSV110), Enterprise/Modular Storage RAID Array (RA/MA6000, RA/MA8000, ESA/EMA12000, and EMA16000), VA and XP disk array systems, Modular Smart Array 1000 (MSA1000), and Modular Smart Array 1500 (MSA1500).
- Manage Secure Path with the Secure Path Manager command line interface (CLI)
- Manage Secure Path for VA and XP with the Auto Path CLI
- Contact technical support for additional assistance

“About this Guide” topics include:

- [Overview](#), page 2
- [Conventions](#), page 3
- [Rack stability](#), page 6
- [Getting help](#), page 7

Overview

This section covers the following topics:

- [Intended audience](#)
- [Related documentation](#)

Intended audience

This book is intended for use by system administrators who are experienced with the following:

- Microsoft Windows NT, Windows 2000, and Windows Server 2003 (32- or 64-bit systems)
- Enterprise Virtual Array 5000 and Enterprise Virtual Array 3000
- Enterprise/Modular Storage RAID Array (RA/MA8000, ESA/EMA12000, and EMA16000) systems
- Modular Smart Array 1000 (MSA1000) and Modular Smart Array 1500 (MSA1500)
- XP256, XP512, XP48, XP128, XP1024, and XP12000 disks arrays
- VA7100, VA7110, VA7400, and VA7410 disk arrays
- Microsoft Cluster Server (MSCS)

Related documentation

In addition to this guide, HP provides corresponding information:

- *HP StorageWorks Secure Path 4.0C Service Pack 2 for Windows and Windows Workgroup Edition Release Notes*
- HP StorageWorks Secure Path Manager HTML Help
- *HP StorageWorks Secure Path Manager 4.0C installation guide*
- *HP StorageWorks Secure Path Manager 4.0C release notes*

Conventions

Conventions consist of the following:

- Document conventions
- Text symbols
- Equipment symbols

Document conventions

This document follows the conventions in [Table 1](#).

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
<i>Italics</i>	Text emphasis and document titles in body text
Monospace font	User input, commands, code, file and directory names, and system responses (output and messages)
<i>Monospace, italic font</i>	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment symbols

The following equipment symbols may be found on hardware to which this guide pertains. They have the following meanings:



Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.



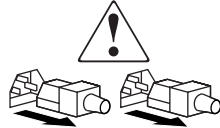
Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack stability

Rack stability protects personnel and equipment.



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - In single rack installations, the stabilizing feet are attached to the rack.
 - In multiple rack installations, the racks are coupled.
 - Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.
-

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our Web site: <http://www.hp.com>.

HP technical support

Telephone numbers for worldwide technical support are listed on the following HP Web site: <http://www.hp.com/support/>. From this Web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage Web site

The HP Web site has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this Web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP Web site for locations and telephone numbers: <http://www.hp.com>.

Installation prerequisites

1

This chapter describes prerequisite information for installing Secure Path for use with the following storage systems:

- Enterprise Virtual Array (HSV100, HSV110)
- Enterprise/Modular Storage RAID Array (RA/MA6000, RA/MA8000, ESA/EMA12000, and EMA16000) systems
- Modular Smart Array (MSA1000/MSA1500) systems
- VA and XP disk arrays

Note: Be sure you complete the tasks in [Table 2](#) before proceeding with the installation.

Secure Path prerequisites

[Table 2](#) lists the system prerequisites for Secure Path 4.0C SP2 installation.

Table 2: Secure Path installation prerequisites

Host Feature	Requirement
Operating systems	Windows NT 4.0 Server and Enterprise Edition Server with SP6a Windows 2000 Server and Advanced Server with Service Pack 3 or Service Pack 4 Windows Server 2003 (x86 and IA64) Windows Server 2003 with Service Pack 1 (x86 and IA64)
Secure Path software kit	StorageWorks Secure Path 4.0C SP2 StorageWorks Secure Path Manager 4.0C
Storage systems	StorageWorks EVA (HSV100, HSV110) StorageWorks EMA12000, ESA/EMA12000 FC, or RA/MA8000/HSG80 StorageWorks dual-redundant MSA1000 and MSA1500 XP256, XP512, XP48, XP128, XP1024, and XP12000 VA7100, VA7110, VA7400, and VA7410
Host Bus Adapters (HBAs)	Refer to the release notes for the latest supported HBAs.
Fibre Channel interconnect hardware	Refer to the <i>HP StorageWorks SAN Design Reference Guide</i> for the latest supported switches at: http://h18006.www1.hp.com/products/storageworks/san/documentation.html

For information about supported storage system software, firmware, and driver versions, refer to the *HP StorageWorks Secure Path 4.0C SP2 for Windows and Windows Workgroup Edition release notes*, part number T3037-98301.

Installation and configuration information

Installation and configuration documentation

Before installing or updating Secure Path, be sure to review the installation and configuration information for your system. The HP Web site has the latest information at: <http://www.hp.com/country/us/eng/prodserv/storage.html>.

Choose **Storage array systems**, click the link for your disk array system, then click **Technical documentation** to view the latest installation and configuration documentation.

Supported SAN topologies

Secure Path for Windows supports SAN topologies as defined and described in the *HP StorageWorks SAN Design Reference Guide*, and other SAN technical documentation. This document is available on the HP Web site at:

<http://h18006.www1.hp.com/products/storageworks/san/documentation.html>.

Choose **SAN Design Guide**.

Installation and configuration checklist

Be sure you complete the following tasks before installing Secure Path:

Table 3: Installation and configuration checklist

Task	
Obtain and review the latest documentation, including release notes, as described in “ Installation and configuration documentation ” on page 11.	<input type="checkbox"/>
Verify receipt of the Secure Path software kit and the Fibre Channel hardware ordered for the installation. If you are missing any component, contact your account representative, or call the HP Customer Service Hotline at (800) 354-9000.	<input type="checkbox"/>
Install all the hardware components as described in the hardware installation and configuration documentation.	<input type="checkbox"/>
Configure the RAID array for multiple-bus failover mode, as described in the hardware documentation. Multiple-bus failover is available on EVA and EMA/ESA/MA/RA arrays only.	<input type="checkbox"/>
Be sure you have the updated drivers for your HBAs, if necessary.	<input type="checkbox"/>
Install the required operating system service packs: Windows NT SP6a Windows 2000 SP3 or SP4 Windows Server 2003 SP1	<input type="checkbox"/>
Close any antivirus programs.	<input type="checkbox"/>
Back up your computer.	<input type="checkbox"/>

Installing Secure Path software

2

This chapter provides installation instructions for Secure Path server software. It describes the installation types and the software installation procedures for Secure Path standalone and cluster configurations. In addition, it describes how to uninstall Secure Path from your system.

Before you begin

Before installing Secure Path:

- Complete the tasks in the “[Installation and configuration checklist](#)” on page 12.
- Be sure you have the following Secure Path CD-ROMs:
 - The Secure Path Manager 4.0C CD-ROM that contains the browser-based Secure Path Manager, the Secure Path Element Manager, and related software.
 - The Secure Path 4.0C SP2 for Windows or Secure Path 4.0C SP2 for Windows Workgroup Edition server software CD-ROM that contains the Secure Path server, driver, and agent software.
- Review the release notes for Secure Path 4.0C SP2 and Secure Path Manager 4.0C.
- Check your Secure Path 4.0C for a Windows license. The license determines on which systems you can install the server software as follows:
 - Full License (part number ending in AA)—no installation restrictions
 - Upgrade license (part number ending in CA)—requires previously installed Secure Path for Windows software (3.1x, 4.0, 4.0A, 4.0B, or 4.0C) for installation
- Log in with Administrator privileges.
- Be sure that no other installation program is in progress when you install Secure Path. For example, if the Found New Hardware wizard is active, close it before you install the Secure Path software.
- Before installing Secure Path software on systems running Microsoft Terminal Server, change the Terminal Server from Execution mode to Installation mode. Installing Secure Path software when the Terminal Server is in Execution mode may have adverse effects on other software products. For detailed information, refer to the Microsoft web site at <http://support.microsoft.com/default.aspx?scid=kb;en-us;186612>.

Software installation types

This section describes the general guidelines for installing the Secure Path server software. Your preparation can vary based on whether Secure Path has been previously installed. In addition, you must have the correct media and license for the type of installation you want. For example, you cannot perform a new installation with the upgrade kit.

Note: It is also possible to install Secure Path software prior to attaching to the hardware.

You can install Secure Path server on systems with:

- New installations (no previously installed versions) on:
 - Standalone systems
 - Cluster configurations
- Upgrade installations on:
 - Standalone systems
 - Cluster configurations

The following sections describe the installation types in detail.

New installations

The following sections describe how to install Secure Path on systems with no previous versions installed. This procedure applies to all supported storage types.

New installations on standalone systems

For a new installation on a standalone system:

1. Perform all hardware setup procedures as described in the hardware installation and configuration documentation that came with your system.
2. Install software solution kits and HBA driver upgrades, if appropriate. (Reboot the system at this time.)
3. Connect a single path to the storage devices.
4. Configure storage sets.
5. Install Secure Path software as described in “[Installing the Secure Path software](#)” on page 22.
6. Shut down and restart the server. The system takes a few seconds to attach the driver to the newly discovered LUNs.
7. Add the redundant paths to the storage devices.

New installations on cluster configurations

Secure Path must be installed on each member of the Microsoft Cluster Server (MSCS) as described in the following procedure.

For new installations on cluster configurations, follow these steps:

1. Perform all hardware setup procedures as described in the hardware installation and configuration documentation.
2. Install software solution kits and HBA driver upgrades, if appropriate. (Reboot the system at this time.)
3. Connect a single path to the storage devices.
4. Configure storage sets.
5. Install Secure Path software as described in “[Installing the Secure Path software](#)” on page 22.
6. Shut down and restart the server.
7. Allow the system to take a few seconds to attach the driver to the newly discovered LUNs before continuing.
8. Add the redundant paths to the storage devices.
9. Install the cluster service on Node A.
10. Perform [step 2](#) through [step 9](#) to install the cluster service on Node B.

11. Repeat for any remaining cluster members.
12. Redistribute disk resources across the cluster nodes.

Upgrading on systems with previous versions of Secure Path

These sections describe how to upgrade the Windows operating system and Secure Path. Use one of the following procedures when upgrading from Secure Path 3.1.X, 4.0, 4.0A, 4.0B, 4.0C SP1, or from Auto Path.

Upgrading from Windows NT 4.0

Secure Path does not support rolling upgrades on Windows NT 4.0 systems. If you are running Windows NT 4.0, perform the following steps:

1. Back up the entire system configuration.
2. Disconnect the server from the SAN connections.
3. Uninstall any existing version of Secure Path or Auto Path, and reboot the server.
4. Perform the Windows operating system upgrade.
5. Install Secure Path 4.0C SP2.
6. Reconnect the server to the SAN.
7. Reboot the system.

Upgrading from Windows 2000 to Windows Server 2003

The following sections provide installation information for Secure Path 4.0C SP2.

Standalone servers

Use the following procedure for standalone servers that boot from direct-connected storage.

1. Back up the entire system configuration.
2. Upgrade to Secure Path 4.0C SP2:
 - If you are currently running an older version of Secure Path, upgrade using the Secure Path 4.0C SP2 for Windows or Secure Path 4.0C SP2 for Windows Workgroup Edition CD-ROM.

- If you are running Auto Path, uninstall the existing version, reboot the server, and then run the Secure Path 4.0C SP2 for Windows or Secure Path 4.0C SP2 for Windows Workgroup Edition installation. Refer to the `Auto Path readme.txt` for deinstallation instructions.
3. Choose one of the following methods to remove all SAN connections from the server to be updated:
 - Unpresent storage to the server.
 - Unplug the Fibre Channel cables.
 - Disable the server's switch ports.
 4. Upgrade the server operating system to Windows Server 2003.
 5. Choose one of the following methods to reconnect the server to the SAN:
 - Enable the server's switch ports.
 - Connect the Fibre Channel cables.
 - Present storage to the server.

Clustered servers

Use the following procedure to upgrade Microsoft Cluster Servers (MSCS) that boot from direct connected storage.

Note: If you are running Secure Path 4.0C SP2 with dynamic load balancing, refer to the *HP StorageWorks Secure Path 4.0C Service Pack 2 for Windows and Windows Workgroup Edition release notes* for the special procedure for this system configuration.

1. Back up your entire system configuration.
2. Using Cluster Administrator, move all cluster shared storage to one server.
3. Using Cluster Administrator, pause the cluster node that you are upgrading.
4. Using Cluster Administrator, for all groups containing resources managed by Secure Path, go to Resource Attributes and disable failback, if enabled.
5. Perform [step 2](#) through [step 4](#) in “[Standalone servers](#)” on page 17 on this cluster node.
6. Using Cluster Administrator, unpause the cluster node that you are upgrading.
7. Repeat [step 2](#) through [step 5](#) for other cluster nodes.

8. Using Cluster Administrator, restore failback settings if necessary and redistribute LUNs across cluster members.

Recovering from an unsuccessful upgrade

Use the following procedure to recover standalone servers that boot from direct-connected storage.

1. Remove all SAN connections from the server to be updated.
2. Reboot to complete the Windows Server 2003 upgrade.
3. Install Secure Path 4.0C SP2 for Windows.
4. Reconnect the server to the SAN.

Upgrading from Windows 2000 to Windows Server 2003 on servers that boot from SAN-connected devices

Use this procedure to upgrade Microsoft Cluster Server (MSCS) systems that boot from SAN-connected storage when upgrading to Secure Path 4.0C SP2 on Windows servers that have one of the following conditions:

- Boot from SAN-connected devices
- Have their `pagefile` located on the SAN
- Have domain controllers that have their Active Directory configuration stored on the SAN

Note: These procedures are for upgrades only. For new installations, follow the procedures in the *HP StorageWorks Booting 32-bit Windows Systems From a Storage Area Network Application Notes*, available on the HP Web site at <http://h18006.www1.hp.com/products/storageworks/san/documentation.html>.

Standalone servers

Use this procedure for standalone servers that boot from SAN-connected storage.

1. Back up your entire system configuration.
2. Upgrade to Secure Path 4.0C SP2 for Windows if you are currently running an older version of Secure Path.

3. Maintain the connection to the boot device, and remove all other SAN connections from the server to be updated using one of the following methods:
 - Unpresent storage to the server.
 - Unplug the Fibre Channel cables.
 - Disable the server's switch ports.
4. Upgrade the server operating system to Windows 2003 Server.
5. Reconnect the server to the SAN:
 - Enable the server's switch ports.
 - Connect the Fibre Channel cables.
 - Present storage to the server.

Clustered servers

Use the following procedure to upgrade Microsoft Cluster Server (MSCS) that boot from SAN-connected storage.

1. Back up your entire system configuration.
2. Using Cluster Administrator, move all cluster shared storage to one server.
3. Using Cluster Administrator, pause the cluster node that you are upgrading.
4. Using Cluster Administrator, for all groups containing resources managed by Secure Path, go to Resource Attributes and disable failback, if enabled.
5. Perform the following steps on the server that does not own any cluster storage:
 - a. Upgrade to Secure Path 4.0C SP2 for Windows if you are currently running an older version of Secure Path.
 - b. Maintain the connection to the boot device, and remove all other SAN connections from the server to be updated using one of the following methods:
 - Unpresent storage to the server.
 - Unplug the Fibre Channel cables.
 - Disable the server's switch ports.
 - c. Upgrade the server operating system to Windows 2003 Server.

- d. Reconnect the server to the SAN:
 - Enable the server's switch ports.
 - Connect the Fibre Channel cables.
 - Present storage to the server.
6. Using Cluster Administrator, unpause the cluster node that you are upgrading.
7. Repeat [step 2](#) through [step 6](#) for other cluster nodes.
8. Using Cluster Administrator, restore failback settings if necessary and redistribute LUNs across cluster members.

Recovering from an unsuccessful upgrade

To recover from an unsuccessful upgrade, restore from the full backup that was performed before starting the upgrade.

Upgrading Secure Path on systems with previous versions of Auto Path

When upgrading Secure Path 4.0C SP2 for Windows on XP or VA disk arrays, you must remove previous versions of Auto Path before you run this installation. Please refer to the Auto Path `readme.txt` for un-installation instructions.

Installing the Secure Path software

This section describes how to install Secure Path Software from the CD-ROM attached to your server, or from a network drive.

To install the Secure Path server software:

1. Access the CD-ROM:
 - If you have AutoRun enabled on your server, the Secure Path setup program starts automatically. Otherwise, Choose **Start > Run**, then browse to the `Launch.exe` program on the CD-ROM drive.
 - If you are accessing the CD-ROM on a Network drive, choose **Start > Run**, then browse to the `Launch.exe` program on the network drive.
2. Follow the on screen instructions to continue with the installation.
3. Indicate whether you want to use an existing configuration file:
 - a. Choose **Yes** to use existing configuration files. If you choose **Yes**, indicate which clients you want to use and click **OK**. The system completes the installation using existing configuration information. Go to [step 4](#).
 - b. Choose **No** to create a configuration file.
4. Click **Password**. The **Password** dialog box displays.
 - a. Enter the old password for the existing configuration files.
 - b. Enter and confirm a new password.

Note: For cluster configurations, be sure the password is the same for each member of the cluster.

5. Click **Add Client**.
6. Enter the name of the client in the **Client** field.
7. Click **OK**.
8. Click **Exit**.
9. Click **Next**.
10. Click **Finish** to complete your Secure Path software installation.

Note: Servers connected to MSA1000 and MSA1500 systems require a second reboot following new 4.0C SP2 installations and following upgrades from Secure Path 3.x.

Using silent installation

Silent installation runs from the CD-ROM on your computer or from a network drive. It installs the Secure Path Server with little intervention. Silent installation is useful if you have a large number of servers that require software installation.

Note: Use silent installation for new installations, modifying a current installation, or for upgrading from a previous version (4.0, 4.0A, or 4.0B to 4.0C, or from 4.0C to 4.0C SP2) and removing the current installation.

Syntax:

```
<install drive>:\SPInstall\setup.exe /s /f1C:\setup.iss  
/f2C:\SPSInstallLog.txt
```

The variable `<install drive>` is the drive that contains the Secure Path installation media.

The variable `setup.iss` is the response file from which you have taken the information for silent installation.

The variable `SPSInstallLog.txt` file records information about the silent installation.

The installation takes a few minutes to complete.

Note: The C: in `/f1C:` and `/f2C:` refers to a local drive on the system or a network drive with write permission on which `SPSInstallLog.txt` can be written. Also, the response file gets created in this drive.

```
<Default_Target_Dir> =  
C:\Program Files\Hewlett-Packard\SecurePath
```

`<User_Target_Dir>` is the directory where you do the new installation. It can also be the directory of an existing installation.

If you need to add clients, do so now by clicking **Start > Programs > Secure Path > SecurePathCfg**.

Silent installation for standard edition

Installing new Secure Path server

To make a new installation, take a backup of the new `.iss` file from the kit and rename it as `setup.iss`. Edit this file to suit the appropriate requirement and use it with the parameter `f1` in the command.

- To install to a directory other than the default directory, edit the `setup.iss` file.
 - Locate `szDir=<Default_Target_Dir>` in line number 23, and then replace it with `szDir=<User_Target_Dir>`.
- For both XP and VA disk array support, edit the `setup.iss` file by replacing:
 - Line 27 with `Sel-0=1`
 - Line 28 with `Sel-1=0`
 - Line 29 with `Sel-2=0`
- For only VA disk array support, edit the `setup.iss` file by replacing:
 - Line 27 with `Sel-0=0`
 - Line 28 with `Sel-1=1`
 - Line 29 with `Sel-2=0`
- For XP and VA disk arrays no support, edit the `setup.iss` file by replacing:
 - Line 27 with `Sel-0=0`
 - Line 28 with `Sel-1=0`
 - Line 29 with `Sel-2=1`
- To avoid the automatic reboot feature, edit the `setup.iss` file by:
 - Locate `Result=6` in line 42, and replace it with `Result=1`
 - Locate `BootOption=3` in line 43, and replace it with `BootOption=0`

Updating installation

To upgrade from a earlier installation, take backup of the `update.iss` file from the kit and rename it as `setup.iss`. Edit this file to suit the appropriate requirement and use it with the parameter `f1` in the command.

- To install to a directory other than the default directory where an earlier version of Secure Path Server was installed, edit the `setup.iss` file by:
 - Locate `Replace szDir=<Default_Target_Dir>` in line number 19, and then replace it with `szDir=<User_Target_Dir>`.
- For XP and VA disk array support, edit the `setup.iss` file by replacing:
 - Line 23 with `Sel-0=1`
 - Line 24 with `Sel-1=0`
 - Line 25 with `Sel-2=0`

For VA disk array support, edit the `setup.iss` file by replacing:

- Line 23 with `Sel-0=0`
 - Line 24 with `Sel-1=1`
 - Line 25 with `Sel-2=0`
- For XP and VA disk arrays no support, edit the `setup.iss` file by replacing:
 - Line 23 with `Sel-0=0`
 - Line 24 with `Sel-1=0`
 - Line 25 with `Sel-2=1`
 - To avoid the automatic reboot feature, edit the `setup.iss` file by:
 - Locate `Result=6` in line 38, and then replace it with `Result=1`
 - Locate `BootOption=3` in line 39, and then replace it with `BootOption=0`

Note: Secure Path Server versions prior to 4.0C SP2 was always installed under `<boot drive>:\Program Files\Compaq\SecurePath`.

Silent installation for workgroup edition

Installing new Secure Path server

To make a new installation, take a backup of the `new.iss` file from the kit and rename it as `setup.iss`. Edit this file to suit the appropriate requirement and use it with the parameter `f1` in the command.

- To install to a directory other than the default directory, edit the `setup.iss` file.
 - Locate `szDir=<Default_Target_Dir>` in line number 23, and then replace it with `szDir=<User_Target_Dir>`.
- For VA disk array support, edit the `setup.iss` file by replacing:
 - Line 27 with `Se1-0=1`
 - Line 28 with `Se1-1=0`
- For no support for VA, edit the `setup.iss` file by replacing:
 - Line 27 with `Se1-0=0`
 - Line 28 with `Se1-1=1`
- To avoid the automatic reboot feature, edit the `setup.iss` file by:
 - Locate `Result=6` in line 41, and replace it with `Result=1`
 - Locate `BootOption=3` in line 42, and replace it with `BootOption=0`

Updating installation

To upgrade from a earlier installation, take backup of the `update.iss` file from the kit and rename it as `setup.iss`. Edit this file to suit the appropriate requirement and use it with the parameter `f1` in the command.

- To install to a directory other than the default directory where an earlier version of Secure Path server is installed, edit the `setup.iss` file by:
 - Locate `szDir=<Default_Target_Dir>` in line number 19, and then replace it with `szDir=<User_Target_Dir>`.
- For VA disk array support, edit the `setup.iss` file by replacing:
 - Line 23 with `Se1-0=1`
 - Line 24 with `Se1-1=0`
- For no support for VA, edit the `setup.iss` file by replacing:
 - Line 23 with `Se1-0=0`
 - Line 24 with `Se1-1=1`
- To avoid the automatic reboot feature, edit the `setup.iss` file by:
 - Locate `Result=6` in line 37, and then replace it with `Result=1`
 - Locate `BootOption=3` in line 38, and then replace it with `BootOption=0`

Note: By default, all the previous versions of Secure Path server versions 4.0C SP2 is installed under <boot drive>:\Program Files\Compaq\SecurePath.

Uninstalling Secure Path server

To uninstall Secure Path Server, make a backup of the `uninstall.iss` file from the kit and rename it as `setup.iss`.

- To avoid the automatic reboot feature, edit the `setup.iss` file by:
 - Locate `Result=6` in line 26, and then replace it with `Result=1`
 - Locate `BootOption=3` in line 27, and replace it with `BootOption=0`

Installing Hs_Service

Hs_Service is a Windows service that collects extended status and error data and generates Application Event Log entries.

Note: Hs_Service supports only RA/MA6000, RA/MA8000, ESA/EMA12000, EMA16000, and EVA.

The Secure Path installation kit installs and starts Hs_Service only if there is an existing Hs_service installed and started on the system. If Hs_Service is not running (that is, it is stopped or disabled), Secure Path installs the service on your system but does not start it.

If Hs_Service was not automatically installed and started during Secure Path installation, you can manually install Hs_Service, open a command prompt window and enter the following command:

```
<installdir>\Hs_Service\Hs_Service.exe -install
```

Note: The variable <installdir> is the folder that you have selected during Secure Path installation.

If Hs_Service was manually installed, it can only be manually removed. To do so, open a command prompt window and enter the following command:

```
"<installdir>\Hs_Service\Hs_Service.exe -remove
```

Note: The variable <installdir> is the folder that you have selected during Secure Path installation.

You can stop the service using the Windows `Services` applet and choosing **Disabled** in the startup type.

Booting Secure Path servers from a Storage Area Network

With the support of external booting with StorageWorks HBAs and RAID arrays, you can optionally eliminate server-based internal boot devices. Booting from an external device provides decreased downtime through faster server replacement in the event of a server failure.

However, booting from a SAN requires specific setup procedures based on the specific software solutions, HBA firmware, and boot BIOS versions. Refer to the following documents for specific information about booting from a SAN:

- For EVA, EMA/ESA/MA/RA, and XP and VA systems, refer to the *HP StorageWorks Booting 32-bit Windows from a Storage Area Network Application Notes* available on the HP Web site at <http://h18006.www1.hp.com/products/storageworks/san/documentation.html>.
- For MSA1000 and MSA1500 systems, refer to *Configuring the StorageWorks MSA1000 and MSA1500 for external boot with Microsoft Windows—new installations* at http://ftp.compaq.com/pub/products/storageworks/techdoc/msa1000/NT_Win2K_extbootsetup.pdf

Uninstalling Secure Path software

This section describes how to uninstall Secure Path software from your system.



Caution: Removal of multi-path software from a multi-path hardware configuration can cause data loss or corruption. Be sure to disconnect the server from multi-path storage or eliminate all but one path to that storage from the server *prior* to removing Secure Path.

Note: You must reconfigure the SAN and reboot your server as part of this procedure. Do not start this procedure unless you can complete all of the following steps without interruption.

To uninstall Secure Path software:

1. Back up all user data on multi-path storage.
2. If possible, disconnect the storage from the server completely. If it is necessary to maintain single-path connections from the server to the storage (as in the case of servers that boot from a SAN device), please consider the following guidelines:
 - a. If this is a simple topology, that is, a one host/one storage array, HP recommends that redundant cable connections be removed.
 - b. If this is a complex topology, that is, the storage continues to be accessed by other servers still in multi-path mode and by this server in single-path mode:
 - For EMA/ESA/MA/RA or MSA systems, use the Storage Management tool of choice to restrict access to the affected LUNs to a single connection (path).
 - For EVA, use switch zoning to establish the single connection (path) from the server.
 - For XP and VA, use switch zoning to establish the single connection (path) from the server.
3. Choose **Start > Settings > Control Panel > Add/Remove Programs**.
4. Choose **StorageWorks Secure Path Server 4.0C SP2**.

5. Choose **Change/Remove** and follow the prompts. The system displays a cautionary statement advising of the potential data loss or corruption which could result from uninstalling Secure Path.
6. Close the Add/Remove Programs window. The LUNs may be inaccessible at this time.
7. Reboot the system.

Managing storage arrays with the Secure Path CLI

3

This chapter describes the user interface for the Secure Path Manager Command Line Utility (CLI) `spmgr`. It includes the following topics:

- [Secure Path Manager CLI overview](#), page 32
- [Starting Secure Path Manager CLI](#), page 35
- [spmgr commands](#), page 36
- [Displaying information](#), page 38
- [Setting storage system properties](#), page 55
- [Path management](#), page 57

Note: Examples are based on the HSV110 controller, but all actions are identical for other controllers.

For information about managing Secure Path with the Web-based interface, refer to the HP StorageWorks Secure Path Manager HTML Help.

Secure Path Manager CLI overview

The Secure Path Manager (`spmgr`) command line interface (CLI) lets you monitor and manage devices, storage systems, and paths to units that are in the Secure Path configuration. It also lets you modify the configuration to repair, replace, or reconfigure. The `spmgr` relies on the Secure Path Agent (`securepathagent`) to handle calls to the Secure Path drivers.

Common terms

[Table 4](#) describes the common `spmgr` terms. For a more complete list of Secure Path terms, refer to the Glossary provided at the end of this guide.

Table 4: Spmgr common terms

Term	Definition
Device	The standard representation for a device or device link on a server. For example: D:
Logical Unit	A device that is managed by Secure Path and identified by its 32-digit World Wide LUN Identifier (WWLUNID).
Storage System Array WWNN	A storage system is identified by its 16-digit World Wide Node Name (WWNN). Note: In the Web-based Secure Path Manager, Storage System Array WWNN is referred to as Subsystem ID .
Controller serial number	The controller is identified by a unique serial number. The serial number of the HSG80 is a 10-character alphanumeric string.

Configuration Information

Path states

[Table 5](#) lists and describes the path states reported by the Secure Path driver.

Table 5: Path states

Path State	Description
Active	Indicates that the path is currently used for the I/O stream.
Available	Indicates that the path is available on the active controller for the I/O stream.
Failed	Indicates that the path is currently unusable for the I/O stream.
Quiesced	Indicates that the path is valid, but has been made unavailable for I/O. Note: In the Web-based Secure Path Manager, Quiesced is referred to as Offline .
Standby	Indicates that the path is valid on the standby controller. Note: In the Web-based Secure Path Manager, Standby is referred to as Available .
Preferred	Indicates that the path is preferred for the I/O stream.

Note: The Preferred path state is recommended for the I/O stream. You cannot assign it to either a Failed or a Quiesced path.

Path Modes

[Table 6](#) lists and describes the path modes reported by the Secure Path driver.

Table 6: Path modes

Path mode	Description
Quiesce	Indicates that a path can be taken offline
Preferred	Indicates that a path can be set as preferred.

Device States

[Table 7](#) lists and describes the device states reported by the Secure Path driver.

Table 7: Device states

Device states	Description
Critical	Only one path remains available to the storage unit.
Degraded	One or more paths are failed to the storage unit
Operational	All paths are available to the storage unit.
Unknown	Unable to communicate with the unit. This may indicate no available path or a failed device.
Failed	Paths are available but an inquiry to the device returns a not-ready state even after retries.

Starting Secure Path Manager CLI

Start the Secure Path Manager CLI from either Windows or a DOS window as follows:

- From Windows, choose **Start > Programs > SecurePath > spmgr**.
- From a DOS window, change directory to:
`<installdir>\SPMgr`

Note: The variable `<installdir>` is the folder that you have selected during Secure Path installation.

Once you have changed to the appropriate directory, you can run `spmgr` commands.

spmgr commands

[Table 8](#) lists the `spmgr` commands and options. Their format and usage are presented and described in the sections following [Table 8](#).

Note: Not all `spmgr` commands are supported on XP/VA. Please refer to [Table 8](#) for additional `spmgr` command information.

Table 8: `spmgr` commands

Command	Options / arguments	Description
<code>spmgr alias</code>	<code>alias_name old_name</code> no argument	Assign an alias to an object.
<code>spmgr display</code>	<code>-c[v] [controller_ser_num]</code> <code>-d[v]</code> <code>-r[v] [WWNN]</code> no argument	Display information about configured Secure Path devices. <i>The -cv option is not supported for XP/VA devices.</i>
<code>spmgr passwd</code>	<code>agent_password</code>	Enter the agent's password.
<code>spmgr quiesce</code>	<code>-p [handle] [path_index]</code>	Temporarily remove selected paths from use. <i>Not supported for XP/VA devices.</i>
<code>spmgr restart</code>	<code>-p [handle] [path_index]</code>	Return a previously quiesced object to an active or available state. <i>Not supported for XP/VA devices.</i>
<code>spmgr repair</code>	<code>-p [handle] [path_index]</code>	Repair one or more failed paths. <i>Not supported on XP/VA devices.</i>
<code>spmgr select</code>	<code>-p [handle] [path_index]</code> <code>-c [handle] [path_index]</code>	Select a path for I/O. Move a LUN to the other controller. <i>The -c option is not supported for XP/VA devices.</i>

Table 8: spmgr commands (Continued)

Command	Options / arguments	Description
spmgr set	-a on off [WWNN] -b on off [WWNN] -b <type> [WWNN] -p on off [WWNN]	Enable or disable special driver properties. Sets LB policy at system level
spmgr unalias	alias_name old_name	Delete an alias.
spmgr version	no argument	Display spmgr, agent, and driver version numbers.

Note: Commands typed without an argument respond with “usage” if the command is a configuration-altering command. The commands `alias`, `display`, and `version` respond with current command or configuration information.

Displaying information

Display header information

Due to the possible complexity of the Secure Path configuration and the possibility of shared storage or clustered software across multiple servers, the display information always has two standard lines of information at the start of the display:

```
Line 1: Server: <Server Name> Report Created: <Date and Time>
Line 2: Command: <Command string>
```

Display differences between controllers

The HSG80, HSV110, XP, and VA array controllers present objects to Secure Path in identical ways. Therefore, there are no differences in the way you manage settings, paths, and devices using the `spmgr`.

The following examples show displays for the different controllers.

HSG80 display

```
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
      2003
Command:spmgr display
Controller Serial Number ZG10506981
Array World Wide Node Name (WWNN) 5000-1FE1-0010-5B00
World Wide LUN ID (WWLUNID)
6000-1FE1-0010-5B00-0009-1050-6981-1234
```

HSV110 display

```
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
      2003
Command:spmgr display
Controller Serial Number P4889B29LC01J
Array World Wide Node Name (WWNN) 5000-1FE1-0015-0AE0
World Wide LUN ID (WWLUNID)
6005-08B4-0001-40BF-0000-A000-1234-0000
```

MSA1000 display

```
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
2003
Command:spmgr display
Controller Serial Number P56350A9IMN0QG
Array World Wide Node Name (WWNN) 500805F3000071C0
World Wide Lun ID (WWLUNID)
6008-05F3-0000-71C0-A501-8890-6C9C-001B
```

XP display

```
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
2003
Command:spmgr display
Controller Serial Number 30132
Array World Wide Node Name (WWNN) 0000003233313033
World Wide Lun ID (WWLUNID)
0000-0000-3630-3030-3442-3537-3135-3430
```

VA display

```
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
2003
Command:spmgr display
Controller Serial Number 00SGR000108X
Array World Wide Node Name (WWNN) 5838303130303052
World Wide Lun ID (WWLUNID)
0030-3930-3030-3030-3030-3043-3030-4755
```

The display command

This section describes the `spmgr display` commands and associated switch parameters. Each switch results in a different type of display.

Note: The verbose flag `[v]` displays detailed information.

Syntax:

```
spmgr display
    -c[v] [controller_ser_num]
    -d[v]
    -r[v] [WWNN]
    (no argument)
```

For each of these command switches, this section presents:

- Description
- Syntax
- All forms of the command
- Examples of all forms of the command
- Example displays of all forms of the command

`spmgr display`

When you enter `spmgr display`, all information for the entire configuration is displayed. The amount of information displayed depends on the number of HBAs, storage systems, and paths to a unit on each storage system.

The full display derives from the component portions described in this section. You can limit the amount of data displayed by combining the `spmgr display` command with one of the described switches.

Example:

```

C:\Program Files\Compaq\SecurePath\SPMgr>spmgr display
Server: hp.mydomain.net Report Created: Tue, Jul 15 17:57:00
2003
Command:spmgr display
=====
Storage: 50001FE15000CC90
Load Balance: Off Auto-restore: On
Path Verify: On
Controller: P66C5D29IO1029
           P66C5D29IO103P
Devices: E: T: U: V: W:
TGT/LUN Device WWLUN_ID Handle #_Paths
0/ 1 E: 0955-0100-B408-0560-0000-1900-0060-0000 2
81ddb0e0
Controller Path_Index HBA Slot # Preferred? Path_Status
P66C5D29IO1029 0 03 no Standby

Controller Path_Index HBA Slot # Preferred? Path_Status
P66C5D29IO103P 1 03 YES Active

TGT/LUN Device WWLUN_ID Handle #_Paths
0/ 2 T: 0955-0100-B408-0560-0000-1E00-0060-0000 2
81dd80e0
Controller Path_Index HBA Slot # Preferred? Path_Status
P66C5D29IO1029 0 03 no Standby

Controller Path_Index HBA Slot # Preferred? Path_Status
P66C5D29IO103P 1 03 YES Active

TGT/LUN Device WWLUN_ID Handle #_Paths
0/ 3 U: 0955-0100-B408-0560-0000-2300-0060-0000 2
81dd50e0

```

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
P66C5D29IO1029	0	03	no	Standby

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
P66C5D29IO103P	1	03	YES	Active

TGT/LUN	Device	WWLUN_ID	Handle	#_Paths
0/ 4	V:	0955-0100-B408-0560-0000-2800-0060-0000	81dd30e0	2

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
P66C5D29IO1029	0	03	no	Standby

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
P66C5D29IO103P	1	03	YES	Active

spmgr display -c[v] [controller_serial_number]

The `-c` switch displays controller-related information. If a parameter is supplied, it must be a `controller_serial_number`. The command has four possible forms:

Syntax:

```
spmgr display      -c
                  -cv
                  -c controller_serial_number
                  -cv controller_serial_number
```

Example:

```
Server: hp.domain.net    Report Created: Tue, Jul 15 18:12:25
2003
```

```
Command: spmgr display -c
```

```
Current Controller List
```

```
= = = = =
```

```
P66C5D29IO1029, P66C5D29IO103P, P4889B49IM403F, P4889B59IM502D,
ZG80900694, ZG90305217
```

Example:

```
spmgr display -cv
= = = = =
Controller: P66C5D29IO1029
Vendor: HP
WWNN: 5000-1FE1-5000-CC90

Controller: P66C5D29IO103P
Vendor: HP
WWNN: 5000-1FE1-5000-CC90
Controller: P4889B49IM403F
Vendor: HP
WWNN: 5000-1FE1-5000-3300
Controller: P4889B59IM502D
Vendor: HP
WWNN: 5000-1FE1-5000-3300
```

Example:

```
spmgr display -c P66C5D29IO1029
= = = = =
Controller: P66C5D29IO1029
Vendor: HP
WWNN: 5000-1FE1-5000-CC90
```

Example:

```
spmgr display -cv P66C5D29IO103P
=====
Controller: P66C5D29IO103P
Vendor: HP
WWNN: 5000-1FE1-5000-CC90
Item  Device    Controller    HBA    Handle    Path Index
=====
0      E:      P66C5D29IO103P    3      81ddb000    1
      WWPN: 5000-1FE1-5000-CC90 Path State: Active [P]
1      T:      P66C5D29IO103P    3      81dd8000    1
      WWPN: 5000-1FE1-5000-CC90 Path State: Active [P]
2      U:      P66C5D29IO103P    3      81dd5000    1
      WWPN: 5000-1FE1-5000-CC90 Path State: Active [P]
3      V:      P66C5D29IO103P    3      81dd3000    1
      WWPN: 5000-1FE1-5000-CC90 Path State: Active [P]
4      W:      P66C5D29IO103P    3      81dd0000    1
      WWPN: 5000-1FE1-5000-CC90 Path State: Active [P]
```

spmgr display -d[v]

The -d switch displays device-related information.

Note: Devices represent LUNs on a storage subsystem.

Syntax:

```
spmgr display    -d
                  -dv
```


Example:

```
spmgr display -d
  Devices by Storage System
=====
Storage:  50001FE15000CC90
Devices:  E:  T:  U:  V:  W:

Storage:  50001FE150003300
Devices:  N:  S:  O:  P:  Q:  R:

Storage:  50001FE100008500
Devices:  F:  G:  H:  I:  J:  K:  L:  M:
```

Example:

```
spmgr display -dv
Device:      E:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE15000CC90
LUNID:       0955-0100-B408-0560-0000-1900-0060-0000
Device:      T:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE15000CC90
LUNID:       0955-0100-B408-0560-0000-1E00-0060-0000
Device:      U:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE15000CC90
LUNID:       0955-0100-B408-0560-0000-2300-0060-0000
Device:      V:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE15000CC90
LUNID:       0955-0100-B408-0560-0000-2800-0060-0000
Device:      W:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE15000CC90
LUNID:       0955-010-B408-0560-0000-2D00-0060-0000
Device:      N:
Status:      Operational [2 paths (1/0/1)]
Storage:     50001FE150003300
```

```

LUNID:      2149-0100-B408-0560-0000-7602-00C0-0000
Device:     S:
Status:     Operational [2 paths (1/0/1)]
Storage:    50001FE150003300
LUNID:      2149-0100-B408-0560-0000-7B02-00C0-0000
Device:     O:
Status:     Operational [2 paths (1/0/1)]
Storage:    50001FE150003300
LUNID:      2149-0100-B408-0560-0000-8002-00C0-0000
Device:     P:
Status:     Operational [2 paths (1/0/1)]
Storage:    50001FE150003300
LUNID:      2149-0100-B408-0560-0000-8502-00C0-0000
Device:     Q:
Status:     Operational [2 paths (1/0/1)]
Storage:    50001FE150003300
LUNID:      2149-0100-B408-0560-0000-8A02-00C0-0000
Device:     R:
Status:     Operational [2 paths (1/0/1)]
Storage:    50001FE150003300
LUNID:      2149-0100-B408-0560-0000-8F02-00C0-0000

```

Note: Secure Path displays path states using the following convention:

[Total number of paths (active/failed/standby)]

Actual numerical equivalents replace the text.

For example, the following attributes are displayed as [10 paths (8/0/2)]:

Total paths = 10, Active = 8, Failed = 0, Standby = 2

spmgr display -r[v] [WWNN]

The `-r` switch displays storage system information. If a parameter is supplied, it must be a WWNN. The command has four possible forms, as shown in the Syntax.

Note: In the Web-based Secure Path Manager, **Storage System Array WWNN** is referred to as **Subsystem ID**.

Syntax:

```
spmgr display -r
                -rv
                -r WWNN
                -rv WWNN
```

Example:

```
spmgr display -r
Server:  hp.mydomain.com Report Created: Wed, Aug 15 15:19:38
2003
Command: spmgr display -r
Storage Systems List
= = = = =
Storage:  50001FE100105B00
Storage:  50001FE1001059F0
```

Example:

```
C:\Program Files\Compaq\SecurePath\SPMgr>spmgr display -rv
Server:  hp.mydomain.net      Report Created: Tue, Jul 15
18:07:50 2003
```

```
Command: spmgr display -rv
```

```
= = = = =
```

```
Storage:  50001FE15000CC90
```

```
Load Balance: Off  Auto-restore: On
```

```
Path Verify: On
```

```
Controller:  P66C5D29IO1029
```

```
              P66C5D29IO103P
```

```
Devices:  E:  T:  U:  V:  W:
```

```
Storage:  50001FE150003300
```

```
Load Balance: Off  Auto-restore: On
```

```
Path Verify: On
```

```
Controller:  P4889B49IM403F
```

```
              P4889B59IM502D
```

```
Devices:  N:  S:  O:  P:  Q:  R:
```

```
Storage:  50001FE100008500
```

```
Load Balance: Off  Auto-restore: On
```

```
Path Verify: On
```

```
Controller:  ZG80900694
```

```
              ZG90305217
```

```
Devices:  F:  G:  H:  I:  J:  K:  L:  M:
```

Example:

```
C:\Program Files\Compaq\SecurePath\SPMgr>spmgr display -r
5000-1FE1-0000-8500

Server:  hp.mydomain.net    Report Created:  Tue, Jul 15
18:09:08 2003

Command: spmgr display -r 50001FE100008500

= = = = =
Storage:  50001FE100008500
Load Balance: Off  Auto-restore: On
Path Verify: On
Controller:  ZG80900694
              ZG90305217
Devices:  F:  G:  H:  I:  J:  K:  L:  M:
```

Example:

```
C:\Program Files\Compaq\SecurePath\SPMgr>spmgr display -rv
5000-1FE1-0000-8500
```

```
Server: hp.mydomain.net    Report Created: Tue, Jul 15
18:09:52 2003
```

```
Command: spmgr display -rv 50001FE100008500
```

```
= = = = =
```

```
Storage: 50001FE100008500
```

```
Load Balance: Off  Auto-restore: On
```

```
Path Verify: On
```

```
Controller: ZG80900694
```

```
ZG90305217
```

```
Devices: F:  G:  H:  I:  J:  K:  L:  M:
```

TGT/LUN	Device	WWLUN_ID	Handle	#_Paths
---------	--------	----------	--------	---------

4/ 11	F:	0085-0000-E11F-0060-B803-9406-9080-0900	2	
-------	----	---	---	--

81dba0e0

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
------------	------------	------------	------------	-------------

ZG80900694	0	03	no	Standby
------------	---	----	----	---------

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
------------	------------	------------	------------	-------------

ZG90305217	0	03	YES	Active
------------	---	----	-----	--------

TGT/LUN	Device	WWLUN_ID	Handle	#_Paths
---------	--------	----------	--------	---------

4/ 12	G:	0085-0000-E11F-0060-CE03-9406-9080-0900	2	
-------	----	---	---	--

81db70e0

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
------------	------------	------------	------------	-------------

ZG80900694	0	03	no	Standby
------------	---	----	----	---------

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
------------	------------	------------	------------	-------------

ZG90305217	1	03	YES	Active
------------	---	----	-----	--------

TGT/LUN	Device	WWLUN_ID	Handle	#_Paths
4/ 13	H:	0085-0000-E11F-0060	C503-9406-9080-0900	2
			81db40e0	

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
ZG80900694	0	03	no	Standby

Controller	Path_Index	HBA Slot #	Preferred?	Path_Status
ZG90305217	1	03	YES	Active

The alias and unalias commands

Secure Path supports the use of aliases. Aliases replace or substitute longer strings for shorter strings.

Example:

The world wide node name (WWNN) of a storage system is 50001FE100053480. You can assign the alias *Bird* to replace the longer, less easy-to-remember WWNN 50001FE100053480.

When an alias is used in an `spmgr` display, it is shown in parenthesis before the term that it substitutes for.

Example:

```
Storage: (fire) 50001FE100013420
```

The alias is `fire`.

Alias commands:

- Define an alias and store it for future use.
- Remove an alias from the alias table.
- Display the alias table.

`spmgr alias alias_name old_name`

To add an alias to the alias table, use the following `spmgr alias` command.

Syntax:

```
spmgr alias_name old_name
```

The following example creates the alias `Birdtop` for the controller serial number: `ZG66654211`.

```
spmgr alias Birdtop ZG66654211
```


spmgr unalias

To remove an alias from the alias table, invoke the `spmgr unalias` command and enter either the `alias_name` or the `old_name`.

Syntax:

```
spmgr unalias  old_name
               alias_name
```

In the following example, the alias, `Birdtop`, is removed from the alias table.

```
spmgr unalias Birdtop
```

spmgr alias

Use the `spmgr alias` command to display the alias table.

Syntax:

```
spmgr alias
```

Example:

```
spmgr alias
Server:  hp.mydomain.com Report Created: Wed, Aug 15 15:42:37
2003
Alias:old_string
= = = = =
beth:5000-1fel-0000-1231
julio:5000-1fel-0000-1233
carmen:ZG111298235442
fredb:ZG238817633215
= = = = =
```

Note:

- When the `spmgr display` is invoked, the screen output uses both the alias, if any, and the standard storage system WWNN or controller serial number. The alias is enclosed in parentheses (`alias_name`).
 - For a command set that requires a parameter, it is assumed that the parameter or its alias may be input. Commands cannot be aliased.
-

The password command

Secure Path requires authentication (entering the agent's password) between the Secure Path agent and `spmgr` before running commands to ensure that only authorized individuals have access to your storage environment. This password

must match the agent's password you entered during installation in the Secure Path Configuration Utility (*SecurePathCfg*). If *spmgr* cannot authenticate the password, you cannot run commands.

`spmgr passwd agent_password`

To enter an agent's password, use the following *spmgr passwd* command.

Syntax:

```
spmgr passwd agent_passwd
```

Setting storage system properties

The `spmgr set` command lets you enable storage system-specific settings for the Secure Path driver:

- **Auto-Restore**—Automatically repairs a failed path.
- **Load Balancing**—Selects the algorithm used for I/O distribution.
- **Path Verification**—Verifies the LUN path state.

The set command

Syntax:

```
spmgr set -a (on | off) [WWNN]
           -b (on | off) [WWNN]
           -b <type> [WWNN]
           -p (on | off) [WWNN]
```

The following sections describe the parameters.

`spmgr set -a on | off [WWNN]`

This command enables or disables the Auto-Restore feature of the driver. When Auto-Restore is enabled, it directs the driver to repair a failed path. When Auto-Restore is disabled, there is no Auto-Restore by the Secure Path driver. The default is disabled.

Note: The **Auto-Restore** cannot be disabled for XP and VA disk arrays. In the Web-based Secure Path Manager, **Auto-Restore** is referred to as **Auto Failback**.

`spmgr set -b on | off [WWNN]`

This command enables or disables the load balancing option of the driver. When load balancing is enabled, it allows I/O to be sent to the unit according to the selected algorithm. The default is Round Robin (**rr**).

`spmgr set -b <type> [WWNN]`

This command enables or disables the load balancing algorithm of the driver. Type is one of the following algorithms: **rr** - Round Robin, **li**—Least I/O, or **lb**—Least Bandwidth.

`spmgr set -p on | off [WWNN]`

This command enables or disables the path verification of the driver. When enabled, this command verifies the state of all possible paths to all units. The default is disabled.

Note: The **Path-Verification** cannot be disabled for XP and VA disk arrays.

Path management

The `spmgr` lets you monitor and manage paths.

The path management tasks include:

- Selecting paths
- Setting paths
- Repairing paths
- Quiescing and restarting paths

Note: On VA and XP disk arrays, only eight paths per device are supported.

The select command

Selecting paths means to identify a path to be used for I/O. Path information can be viewed with one or more options of the `spmgr display` command.

Syntax:

```
spmgr select -p [handle] [path_index]
```

Note: In the Web-based Secure Path Manager, **select -p** is referred to as **make preferred**.

`spmgr select -p [handle] [path_index]`

This command selects the indicated path and makes that path active.

Example:

```
spmgr select -p 8c68e7a 2
```

`spmgr select -c [handle] [controller_serial_number]`

This command moves a LUN unit to the other controller.

Example:

```
spmgr select -C 8c68e7a ZG80900694
```

Note: In the Web-based Secure Path Manager, **select -c** is referred to as **move to other controller**.

The repair command

The `spmgr repair` command lets you repair paths. This command lets you manually repair all or part of a configuration when the Auto-Restore feature has been disabled.

Syntax:

```
spmgr repair -p [handle] [path_index]
```

Example:

```
spmgr repair -p 8c68e7a 3
```

`spmgr repair -p [handle] [path_index]`

This command repairs a path to the indicated storage system.

Syntax:

```
spmgr repair -p [handle] [path_index]
```

Example:

```
spmgr repair -p 8c68e7a 3
```

The quiesce command

Quiescing a path means to move all active I/O from an object to an alternate path.

Syntax:

```
spmgr quiesce -p [handle] [path_index]
```

Note: In the Web-based Secure Path Manager, **quiesce** is referred to as **make offline**.

`spmgr quiesce -p [handle] [path_index]`

When this command is invoked, `spmgr` moves all active I/O using this path to another path on the same controller. The specified path is marked as Quiesced and no further I/O is sent to that path until the path is returned to service with the `restart` command.

You can verify these actions by issuing the `spmgr display` command to view the current path states, as shown in the following example.

Example:

```
spmgr quiesce -p 8c68e7a 3
```

The restart command

Path restarting changes a path to an Available or Standby state. When restarted, the path is available for I/O.

Note: In the Web -based Secure Path Manager, **restart** is referred to as **make online**.

Syntax:

```
spmgr restart -p [handle] [path_index]
```

`spmgr restart -p [handle] [path_index]`

Changes the state to Available or Standby.

Example:

```
spmgr restart -p 8c68e7a 3
```


Managing XP and VA arrays with the legacy Auto Path CLI

4

Secure Path 4.0C SP2 preserves the legacy Auto Path command line interface (CLI) for exclusive use with VA and XP disk arrays. Use the Auto Path CLI only on hosts connected to multipath-capable devices with the Auto Path driver installed. This chapter describes the following information about the commands supported by this interface:

- [Starting Auto Path CLI](#), page 62
- [Auto Path CLI command summary](#), page 63
- [autopath adapters](#), page 64
- [autopath devices](#), page 65
- [autopath help](#), page 66
- [autopath paths device](#), page 67
- [autopath set device](#), page 68

Starting Auto Path CLI

Start the Auto Path CLI from either Windows or a DOS window as follows:

- From Windows, choose **Start > Programs > SecurePath > autopath**.
- From a DOS window change directory to:
`<installdir>\SPMgr`

Note: The variable <installdir> is the folder that you have selected during Secure Path installation.

Once you have changed to the appropriate directory, you can run Auto Path commands.

Auto Path CLI command summary

Table 9 lists the Auto Path CLI commands.

Table 9: Auto Path CLI commands

Command	Options / Arguments	Description
autopath adapters	no arguments	Displays HBAs on the system.
autopath devices	no arguments	Displays detailed information about multi-pathing devices.
autopath help	no arguments	Displays detailed information about an Auto Path CLI command.
autopath paths device	autopath paths device= <i>device_number</i>	Displays the paths to the selected device referenced by the device number.
autopath set device	autopath set device= <i>device_number</i> {policy= <i>policy_name</i> path= <i>path_number</i> }	Sets the load balancing policy for the device specified by the device number.

autopath adapters

This command displays the various host bus adapters (HBAs) in the system.

Example:

HP Auto Path> autopath adapters

Adapter#	Port#	Adapter Name	State	# Paths
1	2	HP HBA-5100x510xPCI	Active	10
2	4	HP HBA-5100x510xPCI	Active	4

autopath devices

This command displays the details of the multipath-capable devices in the system.

Example:

```
HP Auto Path> autopath devices
```

Device#	Device Name		Serial No.	State	Paths	Policy	SCSI address	Disk#
1	HP	OPEN-K	040076E10030	Active	2	RR	0.0.1.0	Disk 1
2	HP	OPEN-K	040076E10031	Active	2	SQB	0.0.2.1	Disk 2
3	HP	OPEN-K	040076E10032	Active	2	NLB	0.0.3.2	Disk 3
4	HP	OPEN-K	040076E10033	Active	2	SQST	0.0.4.3	Disk 4
5	HP	OPEN-K	040076E10034	Active	2	SQST	0.0.5.4	Disk 5
6	HP	OPEN-K	040076E10035	Active	2	SQST	0.0.6.5	Disk 6

autopath help

This command opens the Help for the Auto Path CLI–supported commands.

Example:

```
>autopath help

HP Auto Path for Windows 2000 version x.xx.xx
Copyright (C) Hewlett Packard Inc.
All Rights Reserved.

Displays details of HP Auto Path software supported devices/adapters

AUTOPATH DEVICES          : Displays details of devices
AUTOPATH PATHS DEVICE=#   : Displays details of paths to device#
                           (* at the end of a path signifies that it
is the preferred path)
AUTOPATH SET DEVICE=# PATH=# : Sets preferred path to device# as path#
AUTOPATH ADAPTERS         : Displays details of adapters
AUTOPATH SET DEVICE=# POLICY=<POLICY_NAME> : Sets load balance policy
for device# to <policy_name>

SUPPORTED LOAD BALANCE POLICIES:
  No_Load_Balance (NLB)
  DefaultBalancePolicy (DBP)
  Round_Robin (RR)
  Shortest_Queue_Requests (SQR)
  Shortest_Queue_Bytes (SQB)
  Shortest_Queue_ServiceTime (SQST)

AUTOPATH HELP             : Displays help
```

autopath paths device

This command displays the paths to the selected device referenced by the device number. An asterisk (*) signifies the Preferred path.

Syntax:

```
autopath paths device=device_number
```

device_number is the Auto Path index number shown in the autopath devices command line display.

Example:

The device for this example has a defined load balancing policy.

```
HP Auto Path> autopath paths device=3
Device Name: HP      OPEN-K
Device Serial Number: 040076E10032
```

Path#	Controller Port#	State	Port.Bus.Target.Lun
1	CL-2L	Active	6.4.0.2
2	CL-2L	Active	7.4.0.2 *

autopath set device

This command sets the load balancing policy for the device specified by the device number.

If no load balancing is set for a device, the `autopath set device` command sets the Preferred path to the device.

Syntax:

```
autopath set device=device_number {policy=policy_name |
path=path_number}
```

device_number is the Auto Path index number shown in the **autopath devices** command line display.

policy_name is the load balancing policy name.

path_number is the Preferred path number.

Examples:

```
HP Auto Path> autopath set device=1 policy=round_robin
Device Name: HP      OPEN-3
Device Serial No. : 0400756000E2
Change Load Balance policy (y/n) ? y
Load Balance policy changed. Verify by issuing "autopath" command
```

```
HP Auto Path> autopath set device=1 path=2
Device Name: HP      OPEN-3
Device Serial No.   : 0400756000E2
Controller Port No. : 22
Path Scsi Address   : 3.4.1.0
Change Preferred Path (y/n) ? y
Preferred Path changed. Verify by issuing "autopath" command
```


Software components



This appendix describes the following Secure Path software components included in the Secure Path software kit for Windows 4.0C SP2 and Windows 4.0C SP2 for Workgroup Edition:

- Drivers—Once installed, Secure Path drivers become a critical element of the operating system. Therefore, never uninstall, delete, or disable these drivers while multipathed hardware is attached to the system.
 - **Raidisk.sys** is the Secure Path multipathing driver for Enterprise Virtual Array, Enterprise/Modular Storage RAID Array, and Modular Smart Array. It integrates multipathed hardware to the Windows operating system, provides path management, failure detection, dynamic load balancing, and the reporting of path state information to the Secure Path Manager.
 - **hpap.sys** is the Secure Path multipathing driver that provides the same features provided by **Raidisk.sys** for VA and XP disk arrays.
 - **HszDisk.sys** is a class driver for Windows NT only. This component is installed by the solution software kit, not by Secure Path. It provides unique error handling features and performance enhancements to supported StorageWorks RAID Array controllers. In Windows 2000 and Windows Server 2003, the features provided by HszDisk have been integrated within `raidisk.sys`, precluding the need for this driver. This component is not available with the Workgroup Edition.
 - **rdfil.sys** is a Windows filter driver that provides support for Secure Path with Microsoft clustered servers (MSCS). It also facilitates driver binding for EVA 3000, XP, and VA arrays.

■ Software components

- **Hs_Service** is a Windows service that collects extended status and error data and generates Application Event Log entries for data storage. This service works for the HSG80 and EVA controllers only. Information gathered for EVA controllers is redundant with data passed directly to the StorageWorks Management Appliance. You can disable Hs_Service with the Windows `Services` applet. This component is not available with the Workgroup Edition.
- **Secure Path Agent** is a Windows service that communicates with Secure Path Manager and `spmgr` using the TCP/IP protocol and WinSock API. The agent installs on the host server, along with the Secure Path driver components.
- **The Secure Path Manager CLI** (`spmgr`) is a command line interface that allows you to monitor and manage Secure Path devices, and to change the configuration settings of the drivers. In addition, there is an **Auto Path CLI** for exclusive use with VA and XP disk arrays.
- **Secure Path Manager (SPM)** is a Web-based management utility capable of cross-platform Secure Path configurations. SPM lets you set up multiple path configurations, indicating status of a user-defined set of hosts, storage systems, and paths.

SPM coexists with other utilities such as Insight Manager, or Command View EVA. SPM enables you to efficiently manage your storage systems. Refer to the Secure Path Manager HTML Help for information about using SPM.
- **Secure Path Element Manager (SPEM)** is a component of SPM that communicates directly with Secure Path Agent. For redundancy, you can set up additional SPEMs that reside on other servers.
- **Persistent Reservation Clear Utility** (`spprutil.exe`) removes stray persistent reservations from the device, thereby allowing host systems to access the device.

- **Secure Path registry editing utilities (`sppr_on.reg` and `sppr_off.reg`)** allow RaiDisk to enable (`sppr_on.reg`) or disable (`sppr_off.reg`) dynamic load balancing for MSCS. Load balancing is always enabled on standalone systems.
- **Auto Path registry editing utilities (`appr_on.reg` and `appr_off.reg`)** allow `hpap.sys` to enable (`appr_on.reg`) or disable (`appr_off.reg`) dynamic load balancing for MSCS. Load balancing is always enabled on standalone systems.

Each Secure Path software component uses the Windows Event Log to post error and informational messages.

For more information on the support of dynamic load balancing for MSCS environments, refer to the *HP StorageWorks Secure Path 4.0C SP2 for Windows and Windows Workgroup Edition release notes*, part number T3037–98301.

Secure Path driver event log messages



This appendix lists the `RaidDisk.sys` and `Hpap.sys` Event Log messages, including:

- Messages for Enterprise Virtual Array, Enterprise/Modular Storage RAID Array and Modular Smart Array:
 - [Informational messages for HSV, HSG, and MSA](#), page 74
 - [Warning messages for HSV, HSG, and MSA](#), page 80
 - [Error messages for HSV, HSG, and MSA](#), page 89
- Messages for XP and VA disk arrays:
 - [Informational messages for XP and VA](#), page 95
 - [Error messages for XP and VA](#), page 96

Informational messages for HSV, HSG, and MSA

Informational messages occupy the range of values starting at 513, with the exception of ID 257, a CA-specific recovery case. They provide status information that requires no user intervention.

Event id = 257

Event text

```
FAILSAFE LOCKED: Missing local or remote mirrorset member.  
LUN ID "lunidentifier" has exited the Failsafe Locked state.
```

Description

The controllers have removed the write protected state on this LUN.

Special restrictions

CA systems only.

Event id = 513

Event text

```
The Driver has been started successfully.
```

Description

Does not imply that supported hardware has been found.

Special restrictions

None.

Event id = 514

Event text

```
The Driver has attached a filter device to port "ScsiportN".
```

Description

A startup message. It indicates that Secure Path is ready to service multi-path storage devices if they are available through the HBA known to the OS as ScsiportN.

Special restrictions

Windows NT 4.0 only.

Event id = 515

Event text

The Driver has detected that a previously failed path to Subsystem ID "subsystemidentifier" has been restored.

Dump Data 0 contains the Physical Path Info
<Port | Bus | Target | Lun>.

Dump Data 1 contains the Driver Status.

Dump Data 2 contains the HBA Slot Number
(ffffffff if unavailable).

Description

Path verification or Autofailback has placed a failed path back into the list of available paths. This message is usually displayed for every Restored path to a LUN. If Autofailback is disabled, paths are repaired but not made Active.

Special restrictions

None.

Event id = 516

Event text

The Driver has detected that a previously inaccessible controller to LUN ID "lunidentifier" has been restored.

Dump Data 0 contains Logical Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the Driver Status.

Description

Autofailback has returned the LUN "lunidentifier" to its original owning controller. These messages usually display for each LUN whose owning controller has changed as a result of a failback.

Special restrictions

None.

Event id = 520

Event text

The Driver has detected that LUN ID "lunidentifier" has only a single path.

No extended information in Dump Data.

Description

Only one path has been discovered for the LUN "lunidentifier." The LUN should automatically become Active on this path.

Special restrictions

Windows NT only.

Event id = 521

Event text

The Driver has detected a controller swap on Subsystem ID "subsystemidentifier".

Controller SN "serialnumber1" has been swapped for Controller SN "serialnumber2".

No extended information in Dump Data.

Description

This report is generated after a repair action in which a controller has been replaced.

Special restrictions

None.

Event id = 523

Event text

The Driver has reached it maximum supported Subsystems.
Dump Data 0 contains the value of the Subsystem Limit.

Description

Self-explanatory.

Special restrictions

None.

Event id = 524

Event text

The Driver has recalibrated the performance.
No extended information in Dump Data.

Description

The Secure Path driver maintains certain performance counters to support its load balancing algorithms. This message indicates a maintenance action was performed on the counters. This message could be seen even if load balancing is not enabled.

Special restrictions

None.

Event id = 525

Event text

The Driver has detected an inconsistency in path state.
Dump Data 0 contains the Logical Path Info
< Port | Bus | Target | Lun >.

Description

The driver has detected and corrected a logical inconsistency in its internal path state information.

Special restrictions

None.

Event id = 526

Event text

The Raidisk driver version "N" is being unloaded from the OS possibly to allow an upgrade to another version.

Description

This message may be seen during Secure Path upgrades or uninstall procedures.

Special restrictions

None.

Event id = 527

Event text

The Driver has deleted LUN n, which was previously surprise removed, from its internal tables.

No extended information in Dump Data.

Description

Certain arrays or layered storage software may present and un-present new LUNs fairly frequently, exhausting the driver data storage. This entry indicates that this situation occurred, resulting in the Secure Path driver making some adjustments in its internal data structures.

Special restrictions

Not used in Windows NT.

Event id = 528

Event text

The Driver has load balanced n LUNs on Subsystem ID s.
No extended information in Dump Data.

Description

Following a server boot, when dynamic load balancing is not enabled, the Secure Path driver distributes active path assignments for LUNs across all the available paths.

Special restrictions

None.

Event id = 790

Event text

Currently Secure Path allows only 1 path per controller on MSA.
Subsystem ID is %2.
Dump Data 0 contains Logical Path Info
< Port | Bus | Target | Lun >.

Description

More than two paths were detected to an MSA system. This is not supported by Secure Path; therefore the superfluous connections should be removed. Secure Path stays connected to the MSA using the first path found for both the active and standby controllers.

Special restrictions

None.

Warning messages for HSV, HSG, and MSA

Warning messages occupy the range from 769 to 1023. Although they do not necessarily indicate the need for corrective action, they frequently appear in conjunction with hard errors. Corrective action should be performed in the context of the accompanying errors.

Event id = 769

Event text

The Driver has detected excessive path transitions on LUN ID "lunidentifier". Failover/Failback disabled until next time No extended information in Dump Data.

Description

This message is encountered when failover/failbacks on the LUN *lunidentifier* exceed a specified rate indicating that an intermittent fault on the original owning controller is causing the LUN to be ping-ponged between the controllers. If an additional failover occurs, the LUN will not failback again until the remainder of the current time quantum expires.

Special restrictions

None.

Event id = 770

Event text

The Driver has detected excessive path transition failures on LUN ID "lunidentifier". Failover/Failback disabled until next time quantum.

No extended information in Dump Data.

Description

This message is encountered if a hardware failure causes the LUN *lunidentifier* to fail an ownership change during automated failover/failback. If the underlying fault condition is not corrected, data loss may ensue.

Special restrictions

None.

Event id = 771

Event text

The Driver has restored Failover/Failback operation to LUN ID "lunidentifier".

No extended information in Dump Data.

Description

If either of the excess transition conditions occurred, this message indicates the expiration of the time quantum, allowing normal failover/failback operation to resume.

Special restrictions

None.

Event id = 772

Event text

The Driver has changed access to LUN ID "lunidentifier" to controller SN "controlleridentifier". This was the result of information provided by the subsystem.

No extended information in Dump Data.

Description

"Group" LUN ownership has been transferred to the other controller because of command termination status received from the controller (as opposed to path faults resulting in a "failover"). This message may be presented for LUNs in a controller "group" (such as snapshots, association sets, or controller-based partitions) whose ownership has transferred automatically as a result of a failure detected on one group member.

For grouped LUNs, Secure Path marks failed paths (and logs path failed events) only for the first LUN in the group to detect the failed paths. Remaining group members will have this message posted.

Special restrictions

None.

Event id = 773

Event text

The Driver has changed access to LUN ID "lunidentifier" to controller SN "serialnumber". This was the result of persistent Not Ready status reported.

No extended information in Dump Data.

Description

Not used.

Special restrictions

None.

Event id = 774

Event text

The Driver has been started, but with initialization warnings.

Dump Data 0 contains the Driver Status.

Description

This message indicates internal driver initialization errors, including possible operating system problems such as inability to allocate requested memory.

Special restrictions

Windows NT only.

Event id = 775

Event text

The driver failed to configure LUN/PATH due to an inconsistency in the LUN value on alternate paths.

Dump Data 0 contains the Phys Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the HBA Slot Number
(ffffffff if unavailable).

Description

LUN numbers reported on multiple paths are not the same. This may be a benign condition for EVA systems if you have configured multiple HBAs with Host WWID.

Special restrictions

Windows NT only.

Event id = 776

Event text

```
The Driver failed to configure LUN/PATH due to Inquiry command failure.
```

```
Dump Data 0 contains the Phys Path Info  
< Port | Bus | Target | 0 >.
```

```
Dump Data 1 contains the HBA Slot Number  
(ffffffff if unavailable).
```

Description

The driver was notified that a path exists to a specific LUN. The driver's attempt to issue a status retrieving command on that path has failed. Fault tolerance may be compromised.

Special restrictions

None.

Event id = 777

Event text

```
The Driver failed to allocate a LUN_INFO structure.
```

```
Dump Data 0 contains the Phys Path Info  
< Port | Bus | Target | 0 >.
```

```
Dump Data 1 contains the HBA Slot Number  
(ffffffff if unavailable).
```

Description

A critical memory allocation request has failed. Secure Path cannot provide multi-path access to the specified LUN. Data integrity for this LUN is compromised.

Special restrictions

None.

Event id = 778

Event text

The Driver encountered a LUN whose value exceeds the current maximum.

Dump Data 0 contains the Phys Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the HBA Slot Number
(ffffffff if unavailable).

Description

A physical device returned a LUN number whose value exceeds Secure Path's established upper limit.

Special restrictions

None.

Event id = 779

Event text

The Driver has encountered an I/O Error and will retry.

Dump Data 0 contains the Srb Status.

Description

Self-explanatory.

Special restrictions

This message is returned only for HSG80 LUNs in transparent failover mode.

Event id = 780

Event text

The Driver has encountered an error configuring a subsystem.

Dump Data 0 contains the Phys Path Info
< Port | Bus | Target | 0 >.

Dump Data 1 contains an instance code.

Dump Data 2 contains the HBA Slot Number
(ffffffff if unavailable).

Description

The driver cannot allocate necessary resources to support a new subsystem, or it cannot perform necessary communication with controllers, or the maximum number of subsystems supported by this version of Secure Path may have been exceeded.

Special restrictions

None.

Event id = 781

Event text

The Driver has detected that Subsystem ID "subsystemidentifier" is non-redundant.

No extended information in Dump Data.

Description

The subsystem is reporting that the redundant controller is not present or is not functional.

Special restrictions

MSA1000 and MSA1500 only.

Event id = 782

Event text

The Driver has detected that Subsystem ID "subsystemidentifier" has no active path. The Driver is changing the active path to Controller SN "serialnumber".

No extended information in Dump Data.

Description

The only paths found are to the standby controller. The driver will automatically make the standby controller Active.

Special restrictions

MSA1000 and MSA1500 only.

Event id = 784

Event text

The Driver was unable to obtain the HBA slot number for ScsiPort "portnumber".

No extended information in Dump Data.

Description

Secure Path attempts to display HBA slot number information for ease of maintenance. This information is obtained indirectly by Secure Path from other system components, but not all vendors or HBA model types return necessary information.

Special restrictions

None.

Event id = 785

Event text

The Driver was unable to obtain the HBA type for ScsiPort "portnumber".

No extended information in Dump Data.

Description

Secure Path attempts to display HBA model information for ease of maintenance.

Special restrictions

None.

Event id = 786

Event text

The Driver has detected an unsupported HBA type for ScsiPort%2.

No extended information in Dump Data.

Description

In V 4.0, Secure Path compared the HBA type to a list of "known" HBAs. This message was presented if the HBA discovered was of a type not on the list. Secure Path Version 4 still connects to multi-path storage presented on this HBA.

Special restrictions

None.

Event id = 787

Event text

The Driver was unable to successfully start the Resync Thread.

Dump Data 0 contains the Driver Status.

Description

This message indicates a system resource problem, most commonly memory allocation.

Special restrictions

None.

Event id = 788

Event text

A failure due to grouping might have been encountered.

A mutually exclusive fault between paths to the host might prevent the luns from being able move to the correct controller.

This problem can be fixed by restoring the paths which are broken.

Description

This message most commonly occurs when grouped LUNs are accessible only through different controllers to different hosts. This message should appear on the host that has conceded access to its LUN(s) so that the entire group does not continue to thrash.

Special restrictions

None.

Error messages for HSV, HSG, and MSA

Event id = 256

Event text

FAILSAFE LOCKED: Missing local or remote mirrorset member.
LUN ID "lunidentifier" has entered the Failsafe Locked state.

Description

This message indicates that the controllers have made this LUN *write protected* due to a break in the integrity of the remote copy set.

Special restrictions

CA configurations only.

Event id = 1025

Event text

The Driver has failed initialization.
Dump Data 0 contains the Driver Status.

Description

Severe system resource problems prevent Raidisk from operating in any way.

Special restrictions

None.

Event id = 1026

Event text

The Driver has detected a path failure to Subsystem ID "subsystemidentifier".

Dump Data 0 contains the Phys Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the Driver Status.

Dump Data 2 contains the HBA Slot Number
(ffffffff if unavailable).

Dump Data 3 contains extended Driver Status.

Description

The path identified in the longword at offset 0x28 of the data field of this message has been marked as a failed path by Secure Path. The HBA slot number correlates the *port* in the above path information to the physical location in the server. Other information provided is descriptive only to engineering.

Special restrictions

None.

Event id = 1027

Event text

The Driver has detected a path failure to LUN ID "lunidentifier" during ownership change to controller SN "controlleridentifier".

Dump Data 0 contains the Phys Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the HBA Slot Number
(ffffffff if unavailable).

Description

Not used.

Special restrictions

None.

Event id = 1028

Event text

```
Device failover has been performed to controller SN
"controlleridentifier".

Dump Data 0 contains Logical Path Info < Port | Bus | Target |
Lun >.

Dump Data 1 contains the Driver Status.

Dump Data 2 contains the HBA Slot Number (ffffffff if
unavailable).

Dump Data 3 contains extended Driver Status.
```

Description

Secure Path has successfully transferred the LUN to the other controller as identified in the message text. The path identified in the longword at offset 0x28 of the data field of this message is the last failed path on the inaccessible controller. The HBA slot number correlates the *port* in the above path information to the physical location in the server. Other information provided is descriptive only to engineering.

Special restrictions

None.

Event id = 1029

Event text

```
The Driver has changed access to LUN ID "lunidentifier" to
controller SN "controlleridentifier". This was the result of
the subsystem reporting unavailable status.

No extended information in Dump Data.
```

Description

Not used.

Special restrictions

None.

Event id = 1030

Event text

An attempted path/controller failover for LUN ID "lunidentifier" to controller SN "controlleridentifier" was not successful. This device may be inaccessible.

Dump Data 0 contains Physical Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the Driver Status.

Dump Data 2 contains the HBA Slot Number (ffffffff if unavailable).

Dump Data 3 contains extended Driver Status.

Description

Secure Path determined all paths to the original owning controller had failed, but was unsuccessful in transferring the specified LUN to the other controller. Secure Path attempts to access the LUN on its original controller. As noted, the device is most likely inaccessible if this error is reported.

Special restrictions

None.

Event id = 1031

Event text

An attempted path/controller failback for LUN ID "lunidentifier" to controller SN "controlleridentifier" was not successful. The path/controller may still be inoperative.

Dump Data 0 contains Physical Path Info
< Port | Bus | Target | Lun >.

Dump Data 1 contains the Driver Status.

Dump Data 2 contains the HBA Slot Number
(ffffffff if unavailable).

Description

Dump Data 3 contains extended Driver Status. Auto-failback has exhausted its retries in an attempt to restore the specified LUN to its original owning controller after determining that failed paths to that controller appeared to have been repaired.

Special restrictions

None.

Event id = 1032

Event Text

The Driver has encountered a fatal memory allocation error.

Dump Data 0 contains the Driver Status.

Description

Self-explanatory.

Special restrictions

None.

Event id = 1033

Event Text

The Driver has given up trying this I/O packet

Dump Data 0 contains the Srb Status.

Description

All attempts to deliver an I/O to a LUN have terminated in error and the error recovery budget has been expended.

Special restrictions

HSG80 transparent failover LUNs only.

Event id = 1034

Event Text

Error occurred while sending associated bus reset.

Description

The driver received a bus reset request and must map the original path to the *associated* paths for the LUN. The attempt to issue bus reset down the corresponding path has failed. This condition may result in cluster resource problems such as LUNs being moved to the other cluster node.

Special restrictions

None.

Event id = 1035

Event Text

Error occurred while sending bus reset to break reservation on HBA path failure.

Description

The attempt to issue bus reset down the corresponding path has failed. This condition may result in cluster resource problems such as LUNs being moved to other cluster node.

Special restrictions

None.

Event id = 1036

Event Text

The Driver was unable to successfully start the Bus Reset Thread.

Dump Data 0 contains the Driver Status.

Description

This error is the result of a failed memory allocation request.

Special restrictions

None.

Informational messages for XP and VA

The following messages are specific to XP and VA disk arrays.

There are two informational messages with Event ID values 3 and 4. They provide status information that requires no user intervention.

Event id = 3

Event Text

```
Discovered a new Auto Path capable disk %1; first path SCSI  
address %2.
```

Description

Secure Path has discovered a new multipath device. The SCSI addresses of the device and its first path are contained in the message.

Special restrictions

None.

Event id = 4

Event Text

```
A new path, SCSI address %2 was added to existing Auto Path  
capable disk %1.
```

Description

Secure Path has discovered a new path to an existing multipath device. The SCSI addresses of the device and the new path are contained in the message.

Special restrictions

None.

Error messages for XP and VA

Error messages for XP and VA disk arrays can have Event ID values of 1, 2, and 5 through 8.

Some of the messages indicate hard errors. Perform corrective action in the context of these errors.

Event id = 1

Event Text

An unrecoverable path failure occurred on SCSI address %2.

Device %1 is still accessible over the redundant path(s).

Description

Secure Path detects a failure of a redundant path to an existing multipath device. The SCSI address of the failed path is contained in the message.

Secure Path performs automatic failover to the surviving path(s)

Special restrictions

None.

Event id = 2

Event Text

An unrecoverable path failure occurred on SCSI address %2.

Device %1 failed due to no redundant paths available.

Description

Secure Path detects a failure of the last path to an existing multipath device. The SCSI address of the failed path is contained in the message.

Special restrictions

None.

Event id = 5

Event Text

Too many paths for disk %1, SCSI address %2 was NOT added!

Description

The number of paths discovered to an existing multipath device exceeds the number of supported paths. The message contains the SCSI address of the path discovered in excess of the supported paths.

All paths discovered in excess of the supported paths are masked from the operating system by Secure Path.

Special restrictions

None.

Event id = 6

Event Text

```
The number of devices discovered has exceeded the supported
limit.
```

```
The device (path SCSI address %2) will not be supported by Auto
Path.
```

Description

The number of multipath devices discovered exceeds the number of devices supported by Secure Path.

All multipath devices discovered in excess of the supported devices will not be managed by Secure Path. They will be directly exposed to the operating system.

Special restrictions

None.

Event id = 7

Event Text

```
The path with SCSI address %2 for disk %1 stopped supporting
persistent reservations!
```

Description

A path to an existing multipath device stops recognizing persistent reservation commands. The SCSI address of the particular path is contained in the message.

This message is logged only when the persistent reservation feature in Secure Path (for MSCS environments) is turned on.

Special restrictions

None.

Event id =8

Event Text

One or more paths to disk %1 do not support persistent reservations.

Use of persistent reservations for the disk will be discontinued.

Description

Secure Path finds that one or more paths to an existing multipath cluster device do not support persistent reservations. In this case, Secure Path attempts to switch back to using SCSI reservations for this device.

This message is logged only when the persistent reservation feature in Secure Path (for MSCS environments) is turned on.

Special restrictions

None.

Glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

controller

A hardware device that facilitates communication between a host and one or more LUNs organized as an array.

controller states

- **Critical**—Reported for a controller pair bound in multi-bus failover mode when only one of the controllers is available. This state can mean a failed or offline condition, because the server cannot communicate with the other controller at this time.
- **Operational**—The controller is available with a good status.
- **Unknown**—The server cannot communicate with this controller.

device states

Attributes that describe the current operational condition of a device. A device can exist in the following states:

- **Critical**—Only one path remains available to the storage unit.
- **Degraded**—One or more paths are failed to the storage unit.
- **Operational**—The Secure Path device can be accessed on at least one path.
- **Unknown**—Unable to communicate with the unit. This can indicate no available path or a failed device.
- **Dead**—All paths used by this Secure Path device have failed.

fabric

A network that contains high-speed fiber connections resulting from the interconnection of switches and devices. A fabric is an active and intelligent non-shared interconnect scheme for nodes.

failover

The automatic substitution of a functionally equivalent system component for a component that failed.

HBA

Host Bus Adapter. An I/O device that serves as the interface connecting a host system to the SCSI bus or SAN (Storage Area Network).

host

A computer system on which the Secure Path server software is running.

LUN

Logical Unit Number. The actual unit number assigned to a device at the RAID system controller.

mode

A user-selectable parameter that specifies path behavior during nominal and failure conditions. Paths can be set to one of the following modes:

- **Preferred**—Indicates the desired I/O paths. When Load Distribution is enabled, I/O is distributed to a LUN using all available preferred paths according to a round-robin policy. When path verification is enabled, all preferred paths are verified.
- **Alternate**—Indicates a path that is used only for device access only after all primary paths to the device have failed. Paths in this mode participate in Path Verification, if enabled.
- **Offline**—Indicates a path that will not be used for I/O to a LUN. The Offline mode is logically ordered with one of the other two path modes.

path

A virtual communication route that enables data and commands to pass between a host server and a storage device.

path state

An attribute that describes the current operational condition of a path. A path can exist in one of the following states:

- **Active**—Currently servicing I/O requests.
- **Available**—Available on the active controller for the I/O stream.
- **Failed**—Currently unusable for the I/O stream.
- **Preferred**—indicates the path is preferred for I/O stream, across reboot.

port A

The relative number of an HBA. A specific port number is determined according to its order of discovery by the Windows operating system and includes SCSI, Fibre Channel, and IDE adapter types.

profile

A Secure Path file that stores configuration limits information. The profile includes server, storage system, and failover mode information. The Secure Path Manager lets you create multiple profiles that you can apply to your systems.

SAN

Storage Area Network. A configuration of networked devices for storage.

state

An attribute that describes the current operational condition of an object. *See also* Path, Path State, Attribute, Controller States, and Device States.

target

- For parallel SCSI configurations, the target is the actual target number assigned to a device.
- For Fibre Channel configurations, a target number is assigned by a mapping function at the miniport-driver level and is derived from AL_PA (Arbitrated Loop Physical Addresses) in an FC-AL topology.
- For SAN switched fabric, a target is assigned to a WWPN. This target can have values between 16 and 125.
- For a fabric topology, target is a mapping function derived from the order of discovery according to port connections at the SAN (Storage Area Network) switch.

topology

An interconnection scheme that allows multiple servers and storage devices to communicate. Arbitrated Loop and switched fabric are examples of Fibre Channel topologies.

Index

A

- alias, displaying [53](#)
- appr_off.reg [71](#)
- appr_on.reg [71](#)
- audience [2](#)
- authorized reseller, HP [7](#)
- Auto Path
 - autopath adapters command [64](#)
 - autopath devices command [65](#)
 - autopath help command [66](#)
 - autopath paths command [67](#)
 - autopath set device command [68](#)
 - CLI, starting [62](#)
 - command line interface [70](#)
 - command line interface [61](#)
 - registry editing utilities [71](#)
 - upgrading to Secure Path [21](#)
- Auto-Restore
 - defined [55](#)
 - setting [55](#)

B

- booting from a storage area network [28](#)

C

- checklist, installation and configuration [12](#)
- CLI
 - Auto Path [70](#)
 - Secure Path [70](#)
- cluster services, installing [16](#)
- command line interface
 - Auto Path [61](#)

- Secure Path [32](#)
- commands
 - alias [53](#)
 - Auto Path CLI
 - command summary [63](#)
 - autopath adapters [64](#)
 - autopath devices [65](#)
 - autopath help [66](#)
 - autopath paths [67](#)
 - autopath set device [68](#)
 - display [40](#)
 - display -c controller_serial_number [42](#)
 - display -d [44](#)
 - display -r WWNN [48](#)
 - passwd [54](#)
 - quiesce [58](#)
 - restart [59](#)
 - select [57](#)
 - set [55](#)
 - spmgr summary [35](#)
 - unalias [53](#)
- common terms, spmgr [32](#)
- components
 - Persistent Reservation Clear Utility [70](#)
 - registry editing utilities [71](#)
 - Secure Path agent [70](#)
 - Secure Path Element Manager [70](#)
 - Secure Path Manager [70](#)
 - Secure Path Manager CLI [70](#)
- conventions
 - document [3](#)
 - equipment symbols [4](#)
 - text symbols [3](#)

D

defining, unalias [53](#)

device states [34](#)

devices

displaying in AutoPath [65](#)

setting in Auto Path [68](#)

disk arrays

Secure Path Event log messages [73](#)

software components [69](#)

uninstalling [29](#)

VA [10](#)

XP [10](#)

display command [40](#)

displaying, alias [53](#)

document

conventions [3](#)

prerequisites [2](#)

related documentation [2](#)

drivers

hpap.sys [69](#)

HszDisk.sys [69](#)

raidisk.sys [69](#)

rdfil.sys [69](#)

dynamic load balancing [18](#), [71](#)

E

Enterprise Virtual Array (EVA) [69](#)

Enterprise/Modular Storage RAID Array
(RA/MA6000, RA/MA8000, ESA/EMA12000,
and EMA16000) [69](#), [73](#)

equipment symbols [4](#)

event log messages [73](#)

external booting [28](#)

G

getting help [7](#)

H

help

getting in Auto Path cli [66](#)

help, obtaining [7](#)

host bus adapters

displaying [64](#)

requirements [10](#)

HP

authorized reseller [7](#)

storage web site [7](#)

technical support [7](#)

hpap.sys [69](#)

Hs_Service [27](#), [70](#)

HszDisk.sys [69](#)

I

installation

checklist [12](#)

Hs_Service [27](#)

Microsoft Cluster Server (MSCS) [16](#)

on new standalone systems [16](#)

prerequisites [10](#)

types [15](#)

L

load balancing

defined [55](#)

dynamic [18](#), [71](#)

setting [55](#)

M

messages, event log [73](#)

Microsoft Cluster Server (MSCS) [19](#)

direct-connected storage and [20](#)

new installations [16](#)

upgrading [18](#)

Microsoft Terminal Server [14](#)

modes, path [34](#)

Modular Smart Array 1000 (MSA1000) [69](#), [73](#)

O

operating systems, requirements [10](#)

P

passwords [54](#)

- path
 - management [57](#)
 - modes [34](#)
 - states [33](#)
- Path Verification
 - defined [55](#)
- path verification
 - setting [56](#)
- path_instance
 - quiesce [58](#)
 - select [57](#)
- paths
 - displaying in AutoPath [67](#)
 - quiesce [58](#)
 - repairing [58](#)
 - restarting [59](#)
 - selecting [57](#)
- Persistent Reservation Clear utility [70](#)
- prerequisites [2](#)
- prerequisites, installation [10](#)
- Q**
- quiesce
 - a spmgr [58](#)
 - p spmgr [58](#)
 - paths [58](#)
- R**
- rack stability, warning [6](#)
- raidisk.sys [69](#)
- rdfil.sys [69](#)
- related documentation [2](#)
- restarting paths [59](#)
- S**
- SAN topologies, supported [11](#)
- Secure Path
 - Agents [70](#)
 - command line interface [32](#)
 - components
 - Element Manager [70](#)
 - hpap.sys [69](#)
 - Hs_Service [70](#)
 - HszDisk.sys [69](#)
 - Persistent Reservation Clear utility [70](#)
 - raidisk.sys [69](#)
 - rdfil.sys [69](#)
 - registry editing utilities [71](#)
 - host bus adapters [10](#)
 - installation checklist [12](#)
 - installation prerequisites [10](#)
 - installation types [15](#)
 - Manager [70](#)
 - software components, overview [69](#)
 - spmgr CLI [70](#)
 - uninstalling [29](#)
 - upgrading [17](#)
- SecurePathCfg [54](#)
- selecting paths [57](#)
- set commands [55](#)
 - Auto-Restore [55](#)
 - load balancing [55](#)
 - path verification [56](#)
- spmgr
 - command summary [35](#)
 - common terms [32](#)
 - device states [34](#)
 - display (default) [40](#)
 - display -c controller_serial_number [42](#)
 - display -d [44](#)
 - display -r WWNN [48](#)
 - displaying an alias [53](#)
 - overview [32](#)
 - passwd [54](#)
 - path modes [34](#)
 - path states [33](#)
 - quiesce - a HBA [58](#)
 - quiesce - c path_instance [58](#)
 - quiesce - p path_instance [58](#)
 - repair [58](#)
 - restart -p handle path_index [59](#)
 - select -c handle controller_serial_number [57](#)
 - select -p path_instance [57](#)

- set -a [55](#)
- set Auto-Restore [55](#)
- set -b [55](#)
- set load balancing [55](#)
- set -p [56](#)
- set path verification [56](#)
- starting [35](#)
- unalias [53](#)
- sppr_off.reg [71](#)
- sppr_on.reg [71](#)
- spprutil.exe [70](#)
- standalone systems, installing new [16](#)
- starting
 - Auto Path CLI [62](#)
 - spmgr [35](#)
- states
 - device [34](#)
 - path [33](#)
- storage area network, booting from [28](#)
- storage systems, supported [10](#)
- symbols in text [3](#)
- symbols on equipment [4](#)

T

- technical support, HP [7](#)
- Terminal Server [14](#)
- text symbols [3](#)
- types of installation [15](#)

U

- unalias, defining [53](#)
- uninstalling Secure Path software [29](#)

- upgrading
 - from previous Auto Path versions [21](#)
 - from previous Secure Path versions [17](#)
 - Microsoft Cluster Server (MSCS) [18](#)
- utilities
 - Persistent Reservation Clear [70](#)
 - registry edit [71](#)

V

- VA disk arrays [10](#)
 - drivers [69](#)
 - Secure Path Event log messages [73](#)
 - uninstalling [29](#)

W

- warning
 - rack stability [6](#)
 - symbols on equipment [4](#)
- web sites
 - HP storage [7](#)
- Windows
 - Hs_Service [27](#), [70](#)
 - raidisk.sys [69](#)
 - requirements [10](#)
- Windows NT, HszDisk.sys [69](#)

X

- XP disk arrays [10](#)
 - drivers [69](#)
 - Secure Path Event log messages [73](#)
 - uninstalling [29](#)